



Cyberwarfare and the enterprise: Is the threat real?

by Sherri Davidoff

In early July, there was a great deal of press about a "massive cyber-attack" supposedly originating from North Korea, targeting high-profile South Korean and U.S. websites. The attacks were reportedly launched by "tens of thousands" of infected computers "around the globe," which were used to launch a distributed denial-of-service (DDoS) attack. Oh, and the infected systems were supposed to self-destruct (presumably taking the world with them).

Most security geeks just scratched their heads and wondered how an average-size, rather unsophisticated botnet attack with relatively low impact managed to make it above the fold on the front page of the Wall Street Journal. A few public-facing government websites were slow or inaccessible for a few days, but there were no reports of financial damage or any serious service interruptions.

Sponsored By:



Why all the hype? Is cyberwarfare really something enterprise information security professionals should be concerned about?

The botnet that made headlines last month was tame, but in general, the potential for damage due to cyberwarfare (or cyberaccidents) is huge -- not because of sophisticated enemies, but because our infrastructure is weak and not well maintained. In the U.S., critical infrastructure has come to depend on IT in ways that most people never realize. Skyscraper heating, cooling and access systems can be controlled via the Internet. Hospitals request heart transplants over VoIP phones. Those are just two examples, but there are many others that make it clear that a sophisticated, targeted cyberattack really could cause widespread chaos and even loss of life.

Cyberwarfare is just a small component of a much bigger problem: the need to design a stable, global IT infrastructure. Thoughtless teenagers have wreaked havoc on the Internet countless times without even trying. The Morris Worm of 1988, for example, caused greater devastation than the recent overhyped DDoS attacks, infecting thousands of major Unix machines. Our biggest problem is not that terrorists are out to kill us all, but that even twenty-three years after Morris, our networked infrastructures are about as structurally sound as a Jenga tower.

Even purely accidental network outages have caused major damage to critical infrastructure. Back in 2002, Beth Israel Deaconess Medical Center's network was flooded and brought to a standstill due to an accidental spanning tree loop. Suddenly doctors and lab technicians could not view patient charts, lab results or fill prescriptions over the network. Eventually the emergency room was shut down and patients had to be shuttled to other hospitals. What would happen if someone actually tried to disrupt critical systems using the Internet?

Last year at the SourceBoston security conference, security researcher Dan Geer explored what could have happened with a piece of malware from 2001 called the Nimda virus. Just a few days after September 11, 2001, Nimda spread across the Internet using five different infection vectors, infecting hundreds of thousands of computers within its first day. There is also another, older virus called E911, which caused infected systems to dial 911 over their modems repeatedly. Geer commented that, had the authors of Nimda considered including that functionality in their virulent code, Americans would have "gotten up the morning of Sept. 19 only to find there was no emergency service nationwide; it would have been turned off everywhere and all at once, like a light switch." That would have been just a few days after the nation was already reeling from a crisis.

How to defend against cyberattacks and cyberaccidents

It's hard to know what the next cyber crisis will be, but here are a few best practices that enterprise security teams should consider to avoid becoming victims.

- 1. Prepare for outages.** Map your organization's information flow. Understand what systems/services depend on having critical network functionality. In many cases, companies simply cannot function without the network anymore. We don't have physical pens and paper or staff training to process all of our information. Develop communication and fallback plans for short-term (i.e. 1-hour), medium-term (i.e. 24-hour), and long-term (ie. multiple-day) network outages. Test them out, when possible. Be realistic; plan for what you can, and understand your limitations.

With the economy's current struggles, many businesses do not have the resources to devote to disaster planning. As my mother says, just do your best.

2. Maintain systems. Patch all equipment routinely, including servers, workstations and network equipment. Be sure to include third-party applications. Audit routinely. Collect logs centrally. Even if you don't have time to proactively address disaster recovery, at least make sure to properly maintain the systems you have. Don't be the low-hanging fruit.

3. Share information. This might seem counterintuitive, but we're all in this together. If everyone in a particular industry is seeing the same types of probes or unusual activity, that can help us all identify precursors to incidents and avoid major catastrophes. Sharing information about effective and ineffective defense techniques can help us all respond more efficiently.

4. Be a good neighbor. Don't neglect non-critical systems. Even if there's "nothing important" on that Windows server in the corner, you don't want somebody infecting it and using it to attack other sites.

5. Don't overreact. Huge headlines about yet-another-cyberattack have unnecessarily fueled the fire. Now it seems that a relatively unsophisticated botnet can create global fear and potentially affect international relations, giving malicious individuals yet another incentive. We all have our share of security problems, and cyberwarfare is certainly one. If we all stay cool, however, attackers will have one less reason to launch cyberattacks.

The threat of "cyberwarfare" has been dramatically overhyped, but we are afraid for valid reasons: our national infrastructure is a mess. Accidents have caused just as much damage as "cyberwarfare" or other intentional attacks. "War" is not the problem; mismanagement, disorganization and fear are the real threat.

About the author:

Sherri Davidoff is the co-author of the new SANS class "Sec558: Network Forensics" and author of Philosecurity. She is a GIAC-certified forensic examiner and penetration tester. She provides security consulting for many types of organizations, including legal, financial, healthcare, manufacturing, academic and government institutions.

Buy 2 years of protection for the price of 1

ESET NOD32 Antivirus | **ESET Smart Security**
Business Edition Business Edition

The leaner, faster, superior computer protection



Antispyware



Antivirus



Antispam



Firewall



Go to

www.eset.co.uk/2for1

for full information, T&C's
Offer expires on 31st March 2010.



Resources from ESET



[The Changing Nature of Cybercrime: Attackers, Counter Measures and New Models for Defense-In-Depth](#)

[WWW - World Wide Weaponization](#)

[ESET NOD32 Antivirus 4](#)

About ESET:

ESET provides award winning security solutions that combined fast system scans with the ultimate in proactive protection against both known and unknown online threats. ESET NOD32 Antivirus was awarded "The Best Proactive On-demand Detection" and "The Best Overall Speed Performance" for 2008 by AV Comparatives.

By delivering state-of-the-art endpoint security, ESET Smart Solutions™ increase your security while reducing your TCO. ESET's updated Remote Administrator, delivers a highly scalable enterprise-ready defense against malware, reducing your attack surface resulting in fewer help-desk loads. A light system footprint and blazing fast scanning speed can even extend the useful life of PCs and laptops.

ESET has also been named to the INC500 for the third consecutive year, and has an extensive partner and customer network, including corporations like Intel, Canon, Dell and Microsoft.